

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 10 of 21

**REMARKS**

The present amendment replies to an Office Action dated April 18, 2007. Claims 1, 2, and 4-40 are currently pending in the present application. Claims 10, 16, 19, 23, 25, 29, 31, and 37 have been amended and claims 1, 2, 4-9, 13-15, 21, 22, 27, 28, 34-36, and 40 have been cancelled herein. Claim 3 was cancelled previously. In the Office Action, the Examiner rejected claims 10-39 on various grounds. The Applicants respond to each ground of rejection as subsequently recited herein and respectfully request reconsideration and further examination of the present application.

The Applicants wish to thank Examiner Pich for his interview with the Applicants' attorney on June 5, 2007, and Interview Summary dated June 5, 2007, which completely and accurately records the substance of the interview. As discussed, the Applicants would appreciate the opportunity to have the Applicants' attorney discuss any portions of the specification that could be claimed to obtain an allowance for the case, should the Examiner find that the claims as amended herein are not allowable.

**35 U.S.C. §101**

- A.      Claims 13-15, 21-22, 27-28, and 34-36 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Claims 13-15, 21-22, 27-28, and 34-36 have been cancelled herein to expedite prosecution.

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 11 of 21

35 U.S.C. §103

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references when combined must teach or suggest all the claim limitations. *See MPEP 2143.* The Applicants respectfully suggest that the cited references fail to teach or suggest all the claim limitations.

- B.** Claims 10, 13, and 16 were rejected under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 5,787,172 to Arnold (the *Arnold* patent) in view of U.S. Patent No. 6,748,530 to Aoki (the *Aoki* patent).

The *Arnold* patent and the *Aoki* patent, alone or in combination, fail to disclose, teach or suggest:

as recited in amended independent claim 10, a method for secure communication between a client and a server in a data processing system including an embedded client private key being associated with a client public key generated and stored exclusively outside the client; or

as recited in amended independent claim 16, a computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server including instructions for retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded client private key being associated with a client public key generated and stored exclusively outside the client.

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 12 of 21

As noted by the Examiner, the *Arnold* patent does not disclose the embedded client private key being associated with a client public key stored exclusively outside the client. The *Arnold* patent discloses the MKS generating a public/private signature key pair for its own use, designated the MKS public signature key and the MKS private signature key. The MKS public signature key is programmed into the ROM of each secure chip when the secure chips are manufactured. The MKS personalizes the secure chips for the PS. During personalization, a personalizing unit, such as the MKS here, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. *See column 4, lines 11-27.*

The *Aoki* patent also fails to disclose this element and requires that an individual public key be present at the client for at least part of the certification method, thus storing the individual public key in the client. The Examiner asserts that the client does not store the client's public key and concludes that the client's public key is stored exclusively outside the client. The *Aoki* patent discloses that the temporary registration sub-system generates, in the client 200, a pair of the private key  $M_{is}$  and the public key  $M_{ip}$ . *See column 8, lines 46-48.* The *Aoki* patent also discloses the individual public key created and present at the client during individual temporary registration. *See Figure 23; column 15, lines 58-64.* A group public key is created and present at the client when creating the initial group. *See Figure 25; column 16, lines 25-30.* In addition, the individual public key of the responsible person is required for the encryption of the group private key when adding the responsible person private key to the group. *See column 12, line 65 through column 13, line 1.* The *Aoki* patent is silent as to whether the client retains or disposes of the public keys after use. As noted by the Examiner in the Examiner Interview Summary Record of April 10, 2006, many of the prior art is completely silent as to whether the client retained a copy of its key. The Applicants' specification was amended to make it clear that the embedded client private key being associated with a client public key is stored exclusively outside the client.

Claim 13 has been cancelled herein to expedite prosecution.

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 13 of 21

Withdrawal of the rejection of claims 10 and 16 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent is respectfully requested.

- C. Claims 11, 14, and 17 were rejected under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of U.S. Patent Publication No. US 2002/0078344 to Sandhu, *et al.* (the *Sandhu* publication).

As discussed in Section B above, the *Arnold* patent and the *Aoki* patent fail to disclose, teach, or suggest a client public key generated and stored exclusively outside the client as recited in amended independent claims 10 and 16. The *Sandhu* publication also fails to disclose this element.

Claims 11 and 17 depend directly from independent claims 10 and 16, respectively, and include all the elements and limitations of their respective independent claims. As discussed above, the *Arnold* and *Aoki* patents and the *Sandhu* publication, alone or in combination, fail to disclose a client public key generated and stored exclusively outside the client. Therefore, the *Arnold* and *Aoki* patents and the *Sandhu* publication fail to disclose all the limitations of the rejected claims. The Applicants respectfully submit that claims 11 and 17 are allowable for at least the reasons discussed above for their respective independent claims.

Claim 14 has been cancelled herein to expedite prosecution.

Withdrawal of the rejection of claims 11 and 17 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of the *Sandhu* publication is respectfully requested.

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 14 of 21

**D.** Claims 12, 15, 18, 25, 27, 29, 26, 28, and 30 were rejected under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of the *Sandhu* publication and further in view of U.S. Patent No. 5,970,147 to Davis (the *Davis* patent).

Regarding independent claims 12 and 18, the *Arnold* patent and the *Aoki* patent fail to disclose, teach, or suggest a client public key generated and stored exclusively outside the client as recited in independent claims 10 and 16, as discussed in Section B above. The *Sandhu* publication also fails to disclose this element, as does the *Davis* patent. Claims 12 and 18 depend indirectly from independent claims 10 and 16, respectively, and include all the elements and limitations of their respective independent claims. As discussed above, the *Arnold* and *Aoki* patents, the *Sandhu* publication, and the *Davis* patent, alone or in combination, fail to disclose a client public key generated and stored exclusively outside the client. Therefore, the *Arnold* and *Aoki* patents, the *Sandhu* publication, and the *Davis* patent fail to disclose all the limitations of the rejected claims. The Applicants respectfully submit that claims 12 and 18 are allowable for at least the reasons discussed above for their respective independent claims.

Claim 15 has been cancelled herein to expedite prosecution.

Withdrawal of the rejection of claims 12 and 18 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of the *Sandhu* publication and further in view of the *Davis* patent is respectfully requested.

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 15 of 21

Regarding claims 25, 29, 26, and 30, the *Arnold* patent, the *Aoki* patent, the *Sandhu* publication, and the *Davis* patent, alone or in combination, fail to disclose, teach, or suggest:

as recited in amended independent claim 25, a method for secure communication between a client and a server in a data processing system including retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is generated and stored exclusively outside the client; or

as recited in amended independent claim 29, a computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server including instructions for retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is generated and stored exclusively outside the client.

As noted by the Examiner, the *Arnold* patent does not disclose the embedded client private key being associated with a client public key stored exclusively outside the client. The *Arnold* patent discloses the MKS generating a public/private signature key pair for its own use, designated the MKS public signature key and the MKS private signature key. The MKS public signature key is programmed into the ROM of each secure chip when the secure chips are manufactured. The MKS personalizes the secure chips for the PS. During personalization, a personalizing unit, such as the MKS here, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key.  
*See column 4, lines 11-27.*

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 16 of 21

The *Aoki* patent also fails to disclose this element and requires that an individual public key be present at the client for at least part of the certification method. The Examiner asserts that the client does not store the client's public key and concludes that the client's public key is stored exclusively outside the client. The *Aoki* patent discloses that the temporary registration sub-system generates, in the client 200, a pair of the private key  $M_{is}$  and the public key  $M_{ip}$ . See column 8, lines 46-48. The *Aoki* patent also discloses the individual public key created and present at the client during individual temporary registration. See Figure 23; column 15, lines 58-64. A group public key is created and present at the client when creating the initial group. See Figure 25; column 16, lines 25-30. In addition, the individual public key of the responsible person is required for the encryption of the group private key when adding the responsible person private key to the group. See column 12, line 65 through column 13, line 1. The *Aoki* patent is silent as to whether the client retains or disposes of the public keys after use. As noted by the Examiner in the Examiner Interview Summary Record of April 10, 2006, many of the prior art is completely silent as to whether the client retained a copy of its key. The Applicants' specification was amended to make it clear that the client public key is stored exclusively outside the client.

The *Sandhu* publication also fails to disclose a client public key generated and stored exclusively outside the client, as does the *Davis* patent.

Claims 26 and 30 depend directly from independent claims 25 and 29, respectively, and include all the elements and limitations of their respective independent claims. As discussed above, the *Arnold* and *Aoki* patents, the *Sandhu* publication, and the *Davis* patent, alone or in combination, fail to disclose a client public key generated and stored exclusively outside the client. Therefore, the *Arnold* and *Aoki* patents, the *Sandhu* publication, and the *Davis* patent fail to disclose all the limitations of the rejected claims. The Applicants respectfully submit that claims 26 and 30 are allowable for at least the reasons discussed above for their respective independent claims.

Claims 27 and 28 have been cancelled herein to expedite prosecution.

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 17 of 21

Withdrawal of the rejection of claims 25, 29, 26, and 30 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the *Aoki* patent and further in view of the *Sandhu* publication and further in view of the *Davis* patent is respectfully requested.

- E. Claims 19, 21, 23, 31, 34, and 37 were rejected under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of Examiner's Official Notice and further in view of the *Aoki* patent.

The *Arnold* patent, the *Aoki* patent, and the Examiner's Official Notice, alone or in combination, fail to disclose, teach, or suggest:

as recited in amended independent claim 19, a method for secure communication between a client and a server in a data processing system including retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is generated and stored exclusively outside the client;

as recited in amended independent claim 23, a computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server including instructions for retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is generated and stored exclusively outside the client;

as recited in amended independent claim 31, a method for secure communication between a client and a server in a data processing system including retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key generated and stored exclusively outside the client; or

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 18 of 21

as recited in amended independent claim 37, a computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server including instructions for retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key generated and stored exclusively outside the client.

As noted by the Examiner, the *Arnold* patent does not disclose the embedded client private key being associated with a client public key stored exclusively outside the client. The *Arnold* patent discloses the MKS generating a public/private signature key pair for its own use, designated the MKS public signature key and the MKS private signature key. The MKS public signature key is programmed into the ROM of each secure chip when the secure chips are manufactured. The MKS personalizes the secure chips for the PS. During personalization, a personalizing unit, such as the MKS here, provides the secure chip with a public/private signature key pair, designated the SC public signature key and the SC private signature key. *See column 4, lines 11-27.*

The *Aoki* patent also fails to disclose this element and requires that an individual public key be present at the client for at least part of the certification method. The Examiner asserts that the client does not store the client's public key and concludes that the client's public key is stored exclusively outside the client. The *Aoki* patent discloses that the temporary registration sub-system generates, in the client 200, a pair of the private key  $M_{is}$  and the public key  $M_{ip}$ . *See column 8, lines 46-48.* The *Aoki* patent also discloses the individual public key created and present at the client during individual temporary registration. *See Figure 23; column 15, lines 58-64.* A group public key is created and present at the client when creating the initial group. *See Figure 25; column 16, lines 25-30.* In addition, the individual public key of the responsible person is required for the encryption of the group private key when adding the responsible person private key to the group. *See column 12, line 65 through column 13, line 1.* The *Aoki*

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 19 of 21

patent is silent as to whether the client retains or disposes of the public keys after use. As noted by the Examiner in the Examiner Interview Summary Record of April 10, 2006, many of the prior art is completely silent as to whether the client retained a copy of its key. The Applicants' specification was amended to make it clear that the client public key is stored exclusively outside the client.

Claims 21 and 34 have been cancelled herein to expedite prosecution.

Withdrawal of the rejection of claims 19, 23, 31, and 37 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of Examiner's Official Notice and further in view of the *Aoki* patent is respectfully requested.

F. Claims 20, 22, 24, 32, 35, 38, 33, 36, and 39 were rejected under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of Examiner's Official Notice and further in view of the *Aoki* patent and further in view of the *Sandhu* publication.

As discussed in Section E above, the *Arnold* patent, the *Aoki* patent, and the Examiner's Official Notice fail to disclose, teach, or suggest the client public key being generated and stored exclusively outside the client as recited in amended independent claims 19 and 23; or the embedded client private key being associated with a client public key generated and stored exclusively outside the client, as recited in amended independent claims 31 and 37. The *Sandhu* publication also fails to disclose this element. The *Arnold* patent and the *Aoki* patent also lack a suggestion or motivation to modify or combine their teachings.

Claims 20 and 24 depend directly from independent claims 19 and 23, respectively. Claims 32 and 33 and claims 38 and 39 depend directly or indirectly from independent claims 31 and 37, respectively. The dependent claims include all the elements and limitations of their respective independent claims. As discussed above, *Arnold* patent, the *Aoki* patent, and the Examiner's Official Notice, alone or in combination, fail to disclose a client public key generated and stored exclusively outside the client. Therefore, *Arnold* patent, the *Aoki* patent, and the Examiner's Official Notice fail to disclose all the limitations of the rejected claims.

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 20 of 21

The Applicants respectfully submit that claims 20, 24, 32, 38, 33, and 39 are allowable for at least the reasons discussed above for their respective independent claims.

Claims 22, 35, and 36 have been cancelled herein to expedite prosecution.

Withdrawal of the rejection of claims 20, 24, 32, 38, 33, and 39 under 35 U.S.C. §103(a), as being unpatentable over the *Arnold* patent in view of the Examiner's Official Notice and further in view of the *Aoki* patent is respectfully requested.

July 17, 2007

Case No. AUS920010088US1 (9000/108)

Serial No. 09/833,342

Filed: April 12, 2001

Page 21 of 21

**SUMMARY**

Reconsideration of the rejection of claims 10-12, 16-20, 23-26, 29-33, and 37-39 is respectfully requested in light of the remarks herein. The Applicants submit that claims 10-12, 16-20, 23-26, 29-33, and 37-39 as set forth by this Amendment fully satisfy the requirements of 35 U.S.C. §§ 102, 103, and 112. In view of foregoing remarks, favorable consideration and early passage to issue of the present application are respectfully requested.

Dated: **July 17, 2007**

Respectfully submitted,  
DAVID J. CRAFT, *et al.*

CARDINAL LAW GROUP  
1603 Orrington Avenue, Suite 2000  
Evanston, IL 60201  
(847) 905-7111

/FRANK C. NICHOLAS/

---

Frank C. Nicholas  
Registration No. (33,983)  
Attorney for Applicants